DANIEL L. WARSHAW (Bar No. 185365)
dwarshaw@pwfirm.com
PEARSON WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, California 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

PAUL R. KIESEL (Bar No. 119854)
kiesel@kiesel.law
JEFFREY A. KONCIUS (Bar No. 189803)
koncius@kiesel.law
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, California 90211
Telephone: (310) 854-4444
Facsimile: (310) 854-0812

Attorneys for Plaintiff Steven Cohen

Additional Counsel listed on Signature Page

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, WESTERN DIVISION

STEVEN COHEN on behalf of himself and all others similarly situated,

Plaintiff,

v.

EP GLOBAL PRODUCTION SOLUTIONS, LLC d/b/a ENTERTAINMENT PARTNERS,

Defendant

CASE NO. 2:23-cv-7679

CLASS ACTION

CLASS ACTION COMPLAINT

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Plaintiff Steven Cohen ("Plaintiff"), brings this Class Action Complaint, on behalf of himself and all others similarly situated ("Class Members") against Defendant, EP Global Solutions, LLC d/b/a Entertainment Partners ("EP" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

NATURE OF THE CASE

1. Plaintiff brings this class action against EP for its failure to properly secure and safeguard highly-valuable, protected personally identifiable information, including without limitation, names, Social Security numbers and/or tax identification numbers, and mailing addresses (collectively, "PII"), failure to comply with industry standards to protect information systems that contain PII, and failure to provide adequate notice to Plaintiff and other Class Members that their PII had been accessed and compromised. Plaintiff seeks, among other things, damages, orders requiring EP to fully and accurately disclose the nature of the PII and other information that has been compromised, and to adopt reasonably sufficient security practices and safeguards to protect Plaintiff's and Class Members' PII against future data breaches. Plaintiff further seeks an order requiring EP to provide identity theft protective services to Plaintiff and Class Members for their lifetime, as Plaintiff and Class Members are, and will continue to be at an increased risk of identity theft due to the disclosure of their PII as a result of the conduct of EP described herein.

2. EP provides accounting, management, and finance services to support "every phase of production" in the entertainment industry.[1] These services include, *inter alia*, maintaining Central Casting—a leading background actor database owned

[1] Entertainment Partners, About Us, https://www.ep.com/company/about-us/ (last accessed Aug. 30, 2023).

by EP—as well as processing payroll for over 420,000 production employees.[2] According to its website, EP has more than 1,000,000 end-users worldwide and issues over 9.6 million paychecks annually in North America.[3]

3. EP obtains information about users, including Plaintiff and Class Members, when they register for an account with EP, for Central Casting, or indirectly through the productions for which users are paid. To obtain payment via EP's payroll services, Plaintiff and other users are required to provide their PII to EP.

4. On August 2, 2023, EP filed a notice of data breach with the Attorney General of Maine, announcing it had been subject to a cybersecurity incident in which a "sophisticated threat actor" was able to acquire database files containing users' PII (the "Data Breach").[4] According to EP, cybercriminals acquired the PII of at least 471,362 individuals in the Data Breach.[5]

5. Since the Data Breach, EP provided updates indicating that its investigation revealed the information exposed in the Data Breach included customers' PII.

6. Despite purportedly learning of the Data Breach on June 30, 2023, EP did not begin notifying impacted individuals (including Plaintiff) that their sensitive data was compromised, until August 1, 2023. This delay deprived Plaintiff and Class Members of the opportunity to take meaningful steps to mitigate the impact of the Data Breach.

7. The value of the stolen data, including Plaintiff's and Class Members'

[2] Entertainment Partners, Payroll, https://www.ep.com/payroll/ (last accessed Aug. 30, 2023).

[3] *Id.*

[4] Data Breach Notifications: EP Global Production Solutions, LLC, Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/6dd29d7e-9e44-4ad0-9d48-1e0bd6122ab6.shtml (last accessed Aug. 30, 2023); *see also* Plaintiff's Notice of Data Breach attached as Exhibit A (hereinafter "Notice of Data Breach").

[5] Id.

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

PII, is recognized by EP itself, by cybercriminals who exploit this data to commit identity theft and fraud, and by the individuals, including Plaintiff and Class Members, whose PII was stolen.

8. The Data Breach was a direct and proximate result of EP's failure to implement and follow basic security procedures. Plaintiff's and Class Members' PII is now in the hands of cybercriminals, and Plaintiff and Class Members now face a substantially increased risk of identity theft and other fraudulent activity. This imminent threat will continue for the indefinite future, at least in part because Plaintiff's and Class Members' PII will now be offered and sold to identity thieves in an aggregated format, lending itself, for example, to ease of use in widespread phishing email schemes, identity theft, and other harms caused by the disclosure of PII. Consequently, Plaintiff and Class Members have already and will continue to devote significant time, money and other resources to protect themselves due to EP's actions.

9. Plaintiff on behalf of himself and all others similarly situated, brings claims for negligence, negligence *per se*, breach of contract, invasion of privacy, intrusion upon seclusion, violations of California's consumer and data protection statutes, and claims for declaratory and injunctive relief.

10. Plaintiff seeks damages and injunctive relief requiring EP to adopt sufficient data security practices to safeguard the PII in its custody and control to prevent incidents like the Data Breach from recurring.

11. Because information relating to the Data Breach—including the systems that were impacted and the configuration and design of EP's software and database systems—remains exclusively in EP's custody and control, Plaintiff anticipates that additional information supporting his claims will emerge during discovery.

PARTIES

12. Plaintiff Steven Cohen is a citizen and resident of the State of New Jersey. At some or all times relevant to this Complaint, Plaintiff was a customer of

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

EP. Plaintiff's PII was disclosed without authorization to unknown third parties as a result of the Data Breach. Plaintiff received a Data Breach Notice Letter from EP, dated July 31, 2023, notifying him that his PII had been compromised as a result of the "security incident" EP experienced on June 30, 2023.

13. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time changing passwords, freezing credit cards, and monitoring his various accounts, in an effort to detect and prevent any misuse of his PII – time which he would not have needed to expend but for the Data Breach.

14. As a result of the Data Breach, Plaintiff has been and will continue to be at heightened risk for fraud and identity theft, requiring continued expenditure of time, resources, and attendant damages, for years to come. Such risk is certainly impending and is not speculative, given that information from the Data Breach is now in the hands of cybercriminals seeking to profit from Plaintiff and Class Members' PII.

15. Defendant EP is a Delaware Limited Liability Company with its principal place of business at 2950 North Hollywood Way, Burbank, California, 91505.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

17. Defendant is a Delaware LLC with its principal place of business in Burbank, California. Plaintiff is a citizen of New Jersey. The minimal diversity requirement under CAFA is met.

18. This Court has personal jurisdiction over Defendant pursuant to 28 U.S.C. § 1332(c)(1) because Defendant's principal place of business is in the State of

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

California.

19. Pursuant to 28 U.S.C. § 1391(b)(1), venue is proper in this District because Defendant's principal place of business is in this District and many of Defendant's acts and omissions complained of herein occurred in this District.

FACTUAL BACKGROUND

Entertainment Partners

20. "From production finance to production management," EP provides "integrated, cloud-based digital solutions wherever your business takes you."[6]

21. EP holds itself out to be "the industry leader in Production Finance and Production Management, delivering integrated, cloud-based digital solutions supporting every phase of production."[7]

22. EP is a provider of technology-enabled payroll and production services to the entertainment industry. It serves clients by providing production support services including casting, accounting, payroll, and other financial services in support of film and television productions.

23. On information and belief, EP maintains the PII of customers, clients, employees, and others, necessary to the provision of these services, including, but not limited to:[8]

a. "Contact information, such as name, email address, postal address, and telephone number";

b. "Personal information and security identifiers, such as date of birth and social security numbers";

[6] Entertainment Partners, https://www.ep.com/ (last visited Aug. 30, 2023).

[7] About Us, Entertainment Partners, https://www.ep.com/company/about-us/ (last visited Aug. 30, 2023).

[8] Privacy Notice, Entertainment Partners, https://www.ep.com/legal/privacy-notice/ (last accessed Aug. 30, 2023).

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

c. "Credentials such as a username and password";

d. "Demographic information, such as age and gender"; and,

e. "Financial information, such as credit card, bank account, or other payment information."

24. Consumers are entitled to security for their PII. As a vendor storing sensitive data, EP has a duty to ensure such private, sensitive information is not disclosed or disseminated to unauthorized third parties.

The Entertainment Partners Data Breach

25. According to EP, on the morning of June 30, 2023, an unauthorized third party gained access to the computer network supporting EP's accounting applications.[9]

26. The unauthorized third party accessed, obtained, and exfiltrated files containing customers' names, mailing addresses, Social Security numbers and/or tax identification numbers, and other information provided to EP in connection with prior productions on which those customers worked.[10]

27. According to information presently known, the PII of approximately 471,362 individuals was compromised in the Data Breach.[11]

28. Despite first discovering suspicious activity on June 30, 2023, and "promptly . . . notif[ying] law enforcement," EP waited until August to begin notifying affected individuals that their PII was compromised in the Data Breach.

29. On or about August 1, 2023, EP sent Plaintiff and Class Members a

[9] Notice of Data Breach, Ex. A.

[10] *Id.*

[11] Data Breach Notifications: EP Global Production Solutions, LLC, Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/6dd29d7e-9e44-4ad0-9d48-1e0bd6122ab6.shtml (last accessed Aug. 30, 2023).

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Notice of Data Breach,[12] informing Plaintiff and Class Members:

> **What Happened?** On the morning (Pacific Time) of Friday, June 30, 2023, we detected suspicious activity within a limited area of our computer network that supports a subset of our accounting applications. We promptly took the applications offline, notified law enforcement, and engaged industry-leading cybersecurity experts to investigate. Over the course of the following few weeks, we determined that a sophisticated threat actor evaded our cybersecurity defenses and acquired database files containing your personal information. We have recovered the database files.
>
> **What Are We Doing?** We are continuing to work with federal law enforcement and our cybersecurity experts. We have restored the applications. We will continue to prioritize additional investments in our cybersecurity defenses. We will continue to monitor online forums and marketplaces for any information relating to this event; we have found none to date.
>
> **What Information Was Involved?** The database files included your name, mailing address, social security number and/or tax identification number in connection with prior productions on which you worked. Please note that your compensation information was not affected.

30. The delay between the discovery of the Data Breach and EP's notice deprived Plaintiff and Class Members of the ability to take steps to effectively protect themselves from the impact of the Data Breach.

31. Plaintiff's and Class Members' unencrypted PII is now at risk of being made available for sale on the dark web for purchase by malicious actors, and it may additionally fall into the hands of companies that will use the detailed PII for targeted marketing, without the prior consent of Plaintiff and Class Members. Unauthorized individuals can now easily access Plaintiff's and Class Members' PII.

32. EP failed to use data security practices appropriate to the nature of the sensitive, unencrypted information they accessed, stored and maintained on behalf of

[12] Notice of Data Breach, Ex. A.

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Plaintiff and Class Members.

33. EP knew or should have known that: (i) unauthorized threat actors were targeting financial services companies like EP; and (ii) unauthorized threat actors were aggressive in their pursuit of large companies such as EP.

34. EP, by nature of its business, had cause to be particularly on guard against such attacks.

35. Prior to the Data Breach, EP knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as a result of a cyberattack. Prior to the Data Breach, EP knew or should have known that Social Security numbers and other sensitive data elements within the PII it stored on its networks needed to be encrypted to protect against their publication and misuse in the event of a cyberattack.

Entertainment Partners Obtains, Collects, and Stores Plaintiff's and Class Members 'PII

36. In the ordinary course of doing business with, or receiving services from, EP, Plaintiff and Class Members are regularly required to provide their sensitive, personal, and private protected information (for example, when registering for Central Casting background actor services or to receive payroll services for work on productions that contract with EP).

37. More specifically, EP acknowledges that it "collects information: (i) directly from you when you provide it to us; (ii) automatically when you interact with our Websites and Online Services; and (iii) from third parties such as our clients and business partners."[13]

38. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, EP assumed legal and equitable duties and knew or should

[13] Privacy Notice, Entertainment Partners, https://www.ep.com/legal/privacy-notice/ (last accessed Aug. 30, 2023).

have known it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

39. Plaintiff and Class Members reasonably expect that service providers like EP will use the utmost care to keep their information confidential and secure, to use their information for business purposes only, and to make only authorized disclosures of their information.

40. EP acknowledges its obligation to keep users' PII confidential in its privacy policy, stating "Entertainment Partners and its affiliates ("EP", "we", "us," and "our") are committed to maintaining meaningful privacy protections for all individuals who interact with EP."[14]

41. Despite its professed commitment to "privacy protections," EP failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect unauthorized access to Plaintiff's and Class Members' PII.

42. Had EP remedied the deficiencies in its information storage, computer network, and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, EP could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

The Value of Private Information and Effects of Unauthorized Disclosure

43. EP was well aware that the protected PII it acquires, stores, and maintains is highly sensitive and of significant value to those who would use it for wrongful purposes.

A. <u>The Value of PII</u>

44. PII is property with inherent and sizeable market value. Its value is axiomatic, considering the market value and profitability of "Big Data" corporations

[14] *Id.*

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

in America. Alphabet Inc., the parent company of Google, aptly illustrated this in its 2020 Annual Report, when it reported a total annual revenue of $182.5 billion and net income of $40.2 billion.[15] $160.7 billion of this revenue was derived from its Google business, which is driven almost exclusively by leveraging the PII it collects about the users of its various free products and services.

45. The value of PII is also reflected in criminal law, which recognizes the serious nature of the theft of PII by imposing prison sentences. This strong deterrence is necessary because cybercriminals earn significant revenue from stealing PII. Once a cybercriminal unlawfully acquires personal data, the criminal can demand a ransom or blackmail payment for its destruction, use the information to commit fraud or identity theft, or sell the PII to another cybercriminal on a thriving black market.

46. PII is a particularly valuable commodity to identity thieves when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[16] The purpose of stealing large caches of personal data is to defraud individuals, or to place it for illegal sale and thereby profit from other criminals who buy the data to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information for sale on anonymous websites, making the information widely available to a criminal underworld.

47. There is an active and robust market for this information. As John Sancenito, president of *Information Network Associates*, a company which helps other companies with recovery after data breaches, explained: "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark

[15] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

[16] https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military.

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

web to the people who actually commit the fraud."[17]

48. Thus, Plaintiff and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

49. Once stolen, PII can be used in many different ways. One of the most common is stolen PII being offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and PII. Websites appear and disappear quickly, making it a dynamic environment.

50. The forms of PII exposed in the EP Data Breach are particularly concerning. Unlike credit or debit card numbers—which can quickly be frozen and reissued in the aftermath of a payment card data breach—unique Social Security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of their relationships with government agencies and any number of private companies to update their accounts with those entities.

51. Indeed, even the Social Security Administration ("SSA") warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new

[17] https://www.abc27.com/local-news/york/legislator-security-expert-weigh-in-on-rutters-data-breach/.

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

> number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[18]

52. Social Security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often, Social Security numbers can be used to obtain medical goods or services, including prescription medications. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

B. **Data Breaches Put Consumers at Increased Risk of Fraud and Identity Theft**

53. Cyberattacks and data breaches of financial services companies are especially problematic because of the potentially permanent disruption they cause to the daily lives of their customers. Stories of identity theft and fraud abound, with hundreds of millions of dollars lost by everyday consumers every year as a result of internet-based identity theft attacks.[19]

54. The U.S. Government Accountability Office ("GAO") released a report on data breaches in 2007, finding that victims of identity theft will face "substantial

[18] https://www.ssa.gov/pubs/EN-05-10064.pdf.

[19] Albert Khoury, *Scam alert: 5 most costly data breaches (plus 5 states most targeted)* (July 27, 2022), https://www.komando.com/security-privacy/most-costly-data-breaches/847800/.

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

costs and time to repair the damage to their good name and credit record."[20]

55. The FTC recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[21]

56. Cybercriminals use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

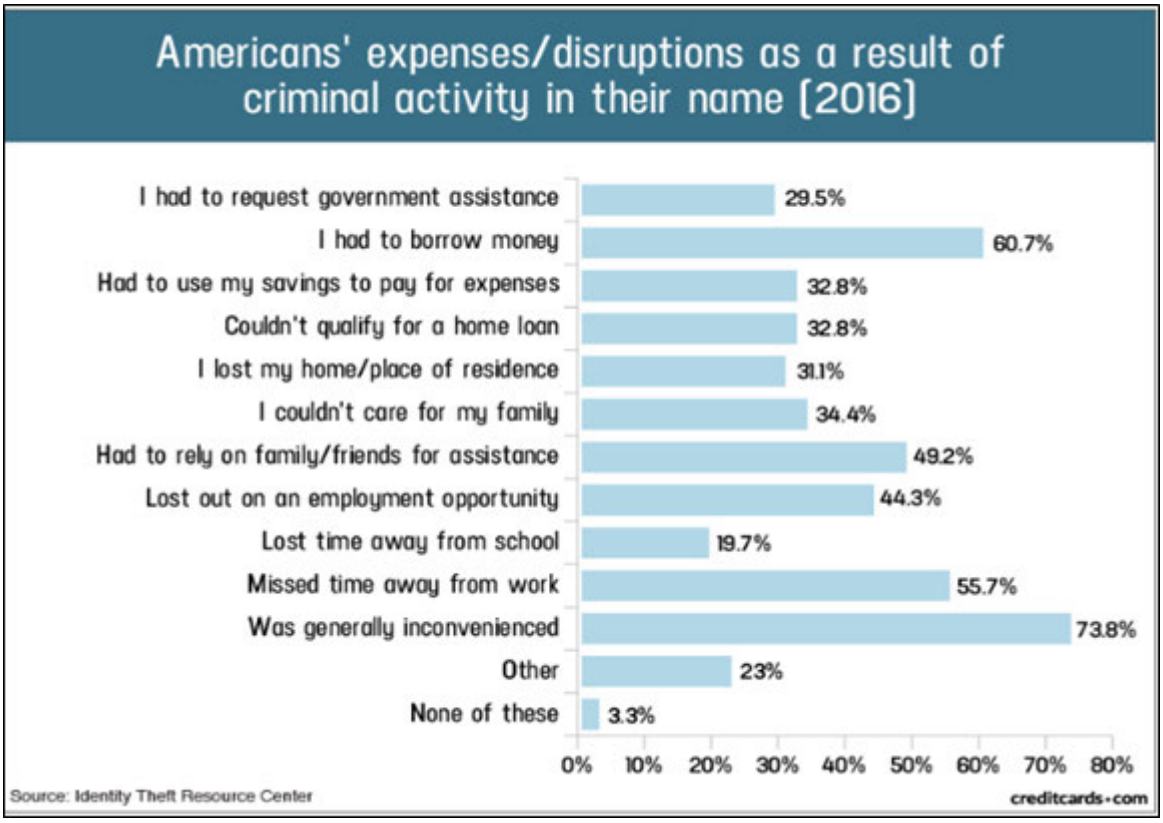
57. Identity thieves can also use Social Security numbers to obtain a driver's license or other official identification card in the victim's name, but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, seek unemployment or other benefits, and may even give the victim's PII to police during an arrest, resulting in an arrest warrant being issued in the victim's name. A study by the Identity Theft Resource Center ("ITRC") shows the multitude of harms caused by fraudulent use of personal and financial information:[22]

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

[20] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

[21] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/Steps (last visited Mar. 23, 2021) [https://perma.cc/ME45-5N3A].

[22] Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (updated Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-



58. As set forth above, 96.7% of study subjects experienced costs or other harms from the criminal activity.[23] As illustrated in the above graphic, this includes devastating results such as "I lost my home/place of residence" and "I couldn't care for my family." Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly one-third of survey respondents had to request government assistance as a result of the identity theft, such as welfare, EBT, food stamps, or similar support systems.[24] The ITRC

theft-fraud-statistics-1276.php [https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php].

[23] *Id.*

[24] *Id.*

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

study concludes that "identity theft victimization has an extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual."[25]

59. The PII exfiltrated in the EP Data Breach can also be used to commit identity theft by placing Plaintiff and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

60. Notably, there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and between when PII and/or financial information is stolen and when it is used. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

61. PII is such an inherently valuable commodity to identity thieves that, once compromised, criminals often trade the information on the dark web for years.

62. Furthermore, data breaches that expose personal data, and in particular non-public data of any kind directly and materially increase the chance that a potential victim will be targeted by a spear phishing attack in the future, and spear phishing

[25] *Id.*

[26] GAO Report, *supra* n.20, at 29.

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

results in a high rate of identity theft, fraud, and extortion.[27]

63. There is a strong probability that entire batches of stolen information from the EP Data Breach have yet to be made available on the black market, meaning Plaintiff and Class Members will remain at an increased risk of fraud and identity theft for many years into the future. Thus, as the respective Notices advise, Plaintiff must vigilantly monitor his financial accounts for many years to come.

64. As a highly sophisticated party that handles sensitive PII, EP failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII.

65. The ramifications of EP's failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data can be sold in small batches to multiple buyers as opposed to in bulk to a single buyer. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts, and Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

66. Thus, EP knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were

[27] *See* Leo Kelion & Joe Tidy, *National Trust Joins Victims of Blackbaud Hack*, BBC News (July 30, 2020), https://www.bbc.com/news/technology-53567699 (concluding that personal information such as "names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware").

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

breached. EP failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

FTC Guidelines

67. EP is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

68. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[28]

69. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect their customers' personal information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[29]

70. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[30]

71. The FTC has brought enforcement actions against businesses for failing

[28] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[29] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136proteting-personal-information.pdf.

[30] *Id.*

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an "unfair act or practice" prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. EP failed to properly implement basic data security practices. EP's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

73. EP was at all times fully aware of its obligations to protect the PII of consumers because of its business model of collecting PII and storing payment information. EP was also aware of the significant repercussions that would result from its failure to do so.

CLASS ACTION ALLEGATIONS

74. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff seeks certification of the Class defined as:

> All individuals in the United States whose PII was compromised in the Entertainment Partners Data Breach which occurred around June 2023.

75. The Class asserts claims against Defendant for negligence, negligence *per se*, declaratory judgment, and breach of express and implied contract as well as for violations of the California Consumer Privacy Act and California Unfair Competition Law.

76. Excluded from the Class is Defendant, its subsidiaries and affiliates, officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

77. Plaintiff reserves the right to modify or amend the definition of the

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

proposed Class, if necessary, before this Court determines whether certification is appropriate.

78. The requirements of Rule 23(a)(1) are satisfied.

79. Numerosity. The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach. The approximate size of the Class is 471,362 individuals as set forth above.

80. Commonality: The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting members of the Class. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII by storing that information unencrypted on computers and hard drives in the manner alleged herein, including

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

failing to comply with industry standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant had respective duties not to use the PII of Class Members for non-business purposes;

i. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

j. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

81. Typicality: The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII. Plaintiff and members of the Class were customers of EP (or EP's clients), each having their PII obtained by an unauthorized third party.

82. Superiority: The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class Members. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the Class Members. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above. While the aggregate damages that may be awarded to the members of the Class are likely to be substantial, the damages suffered by the individual members are relatively

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each Class Member. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class Member.

83. The nature of notice to the proposed class and/or contemplated is by direct communication (mail or email) and publication if found to be necessary.

California Law Should Apply to Plaintiff and the Nationwide Class

84. The State of California has a significant interest in regulating the conduct of businesses operating within its borders. California, which seeks to protect the rights and interests of California and all residents and citizens of the United States against a company headquartered and doing business in California, has a greater interest in the claims of Plaintiff and the Nationwide Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

85. The principal place of business and headquarters of EP, located at 2950 North Hollywood Way, Burbank, California is the "nerve center" of its business activities – the place where its high-level officers direct, control, and coordinate EP's activities, including its data security functions and major policy, financial, and legal decisions.

86. EP's actions leading up to the Data Breach, its response thereafter, and corporate decisions surrounding such response, were made from and in California.

87. EP's breaches of duties owed to Plaintiff and Class Members emanated from California.

88. Application of California law to the Nationwide Class with respect to Plaintiff's and Class Members' claims is neither arbitrary nor fundamentally unfair

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

because California has significant contacts and a significant aggregation of contacts that create a State interest in the claims of Plaintiff and the Class.

89. Specifically, EP's General Terms of Use specifically state that the "the laws of the State of California without regard to choice of law rules and state and federal courts located in Los Angeles County, California will have exclusive jurisdiction over any dispute relating to this Agreement, and each party consents to the exclusive jurisdiction of those courts."

90. Under California's choice of law principles, which are applicable to this action, the common law of California applies to the nationwide common law claims of all Class Members. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, and given that California has the most significant relationship to EP—because it is headquartered in California, EP's computer systems are located in California, as are its executives and officers who made decisions which led to the Data Breach—there is no conflict in applying California law to non-resident consumers such as Plaintiff and the Nationwide Class.

FIRST CAUSE OF ACTION

Negligence

91. On behalf of Plaintiff and the Nationwide Class, Plaintiff repeats and realleges Paragraphs 1-90 as if fully alleged herein.

92. EP owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession and control from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing EP's security systems to ensure that Plaintiff's and Class Members' PII was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

93. EP's duty to use reasonable care arose from several sources, including but not limited to those described below.

94. EP had a common law duty to prevent foreseeable harm to others. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. As a financial services provider collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, EP was obligated to act with reasonable care to protect against these foreseeable threats.

95. EP admits that it has the responsibility to protect the consumer data it is entrusted with, and that it did not live up to its responsibility to protect the PII at issue here.

96. EP breached the duties owed to Plaintiff and Class Members and was therefore negligent. EP breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiff's and Class Members' PII in its possession had been, or was reasonably believed to have been, stolen or compromised.

97. But for EP's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

98. As a direct and proximate result of EP's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with requesting credit freezes;

c. Costs associated with the detection and prevention of identity theft;

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the EP Data Breach;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII, which they entrusted, directly or indirectly, to EP with the mutual understanding that EP would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to theft and misuse of their PII, which remains in EP's possession and is subject to further breaches so long as EP fails to undertake appropriate and adequate measures to protected Plaintiff.

99. As a direct and proximate result of EP's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION

Negligence Per Se

100. On behalf of Plaintiff and the Nationwide Class, Plaintiff repeats and realleges Paragraphs 1-90, as if fully alleged herein.

101. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as EP for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of EP's duty.

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

102. EP violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with industry standards. EP's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

103. EP's violation of Section 5 of the FTC Act constitutes negligence *per se*.

104. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

105. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

106. Additionally, EP has a duty to act reasonably in handling consumer data and to use reasonable data security measures arising under the Gramm–Leach–Bliley Act's implementing regulations, 16 C.F.R. § 314 (the "Safeguards Rule"), which "sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information" and "applies to the handling of customer information by all financial institutions[.]" 16 C.F.R. § 314.1(a)-(b).

107. The Safeguards Rule "applies to all customer information in [a financial institution's] possession, regardless of whether such information pertains to individuals with whom [a financial institution has] a customer relationship, or pertains to the customers of other financial institutions that have provided such information to [the subject financial institution]." 16 C.F.R. § 314.1(b).

108. The Safeguards Rule requires financial institutions and entities who act on behalf of financial institutions to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

are appropriate to [the financial institution's] size and complexity, the nature and scope of [the financial institution's] activities, and the sensitivity of any customer information at issue." 16 C.F.R. § 314.3(a).

109. Specifically, the Safeguards Rule requires entities to:

> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
>
> (1) Employee training and management;
>
> (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
> (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
>
> (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
>
> * * *
>
> (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

16 C.F.R. § 314.4.

110. As alleged herein, EP breached its duties under the Safeguards Rule.

111. EP also has a duty under the California Constitution which contains a Right to Privacy clause, Article 1, Section 1 which states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

defending . . . privacy."[31]

112. EP's failure to implement reasonable measures to secure consumers' PII violates the California Constitution and the FTC Act.

113. As a direct and proximate result of EP's negligence, Plaintiff and Class Members have been injured as described herein and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION

Declaration of Judgment

114. On behalf of Plaintiff and the Nationwide Class, Plaintiff repeats and realleges Paragraphs 1-90, as if fully alleged herein.

115. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

116. An actual controversy has arisen in the wake of the EP Data Breach regarding Plaintiff's and Class Members' PII and whether EP is currently maintaining data security measures adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII. EP's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

117. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

[31] Calif. Const. Art. 1, § 1, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CONS&division=&title=&part=&chapter=&article=I.

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

a. EP owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act; and

b. EP continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

118. This Court should issue corresponding prospective injunctive relief requiring EP to employ adequate data security protocols consistent with law and industry standards to protect consumers' PII.

119. If an injunction is not issued, Plaintiff will suffer irreparable injury in the event of another data breach at EP. The risk of another such breach is real, immediate, and substantial. If another breach at EP occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, forcing Plaintiff and Class members to bring multiple lawsuits to rectify the same conduct.

120. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to EP if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. Conversely, the cost to EP of complying with an injunction and employing reasonable prospective data security measures is relatively minimal. Moreover, EP has a pre-existing legal obligation to employ such measures.

121. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at EP, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

FOURTH CAUSE OF ACTION

Invasion of Privacy

122. On behalf of Plaintiff and the Nationwide Class, Plaintiff repeats and realleges Paragraphs 1-90 as if fully alleged herein.

123. Plaintiff and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored and maintained by EP. Plaintiff and Class

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Members are therefore entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access, as occurred in the Data Breach.

124. Plaintiff and Class Members reasonably expected that EP would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, or disclosed to any unauthorized parties for any improper purpose.

125. EP unlawfully invaded the privacy rights of Plaintiff and Class Members by engaging in the conduct described above, including by failing to protect their PII and by permitting unauthorized third parties to access, exfiltrate and view their PII.

126. This invasion of privacy resulted from EP's failure to properly secure and maintain Plaintiff's and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of the unguarded data.

127. Plaintiff's and the Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it.

128. The disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

129. EP's willful and reckless conduct which, permitted unauthorized access, exfiltration and disclosure of Plaintiff's and the Class Members' sensitive PII, is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

130. The unauthorized access, exfiltration, and disclosure of Plaintiff's and Class Members' PII occurred without their consent, and in violation of various statutes, regulations and other laws.

131. As a result of the invasion of privacy caused by EP, Plaintiff and the Class Members suffered and will continue to suffer damages and injury as set forth herein.

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

132. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

133. Plaintiff and Class Members are entitled to injunctive relief requiring Defendant to: (i) strengthen their data security programs and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide robust and adequate credit monitoring to Plaintiff and Class Members; and any other relief this Court deems just and proper.

FIFTH CAUSE OF ACTION

Breach of Express Contract

134. On behalf of Plaintiff and the Nationwide Class, Plaintiff repeats and realleges Paragraphs 1-90 as if fully alleged herein.

135. Plaintiff and Class Members formed a contract with EP when they obtained products or services from EP.

136. Plaintiff and Class Members fully performed their obligations under their contracts with EP.

137. EP breached the agreement with Plaintiff and Class Members by failing to protect their PII. Specifically, it (i) failed to take reasonable steps to use safe and secure systems to protect Plaintiff's and Class Members' PII; and (ii) disclosed that PII to unauthorized third parties, in violation of the agreement.

138. As a direct and proximate result of EP's breach of contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of their stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by Defendant; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

SIXTH CAUSE OF ACTION

Breach of Implied Contract

139. On behalf of Plaintiff and the Nationwide Class, Plaintiff repeats and realleges Paragraphs 1-90 as if fully alleged herein.

140. When Plaintiff and Class Members provided their sensitive personal information to EP in exchange for services, they entered into implied contracts with EP, under which EP agreed to take reasonable steps to protect their sensitive personal information.

141. EP solicited and invited Plaintiff and Class Members to provide their sensitive personal information as part of its regular business practices. Indeed, to obtain payment from or utilize the casting services provided by EP, EP requires customers to provide sensitive personal information including Social Security numbers. Plaintiff and Class Members accepted EP's offers and provided their sensitive personal information to EP.

142. Plaintiff and Class Members reasonably believed and expected that EP's data security practices complied with relevant laws, regulations, and industry standards when they entered into the implied contracts with EP.

143. Plaintiff and Class Members paid money (directly and/or indirectly) to EP, and Plaintiff and Class Members therefore reasonably believed and expected that

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

EP would use part of those funds to obtain and oversee adequate data security. EP failed to do so.

144. Plaintiff and Class Members would not have provided their sensitive personal information to EP in the absence of EP's implied promise to keep their sensitive personal information reasonably secure.

145. Plaintiff and Class Members fully performed their obligations under the implied contracts by paying money to EP.

146. EP breached its implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures.

147. As a direct and proximate result of EP's breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

148. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

SEVENTH CAUSE OF ACTION

Violation of the California Consumer Privacy Act Cal. Civ. Code §§ 1798.100, *et. seq.* ("CCPA")

149. On behalf of Plaintiff and the Nationwide Class, Plaintiff repeats and realleges Paragraphs 1-90 as if fully alleged herein.

150. California's Consumer Privacy Act ("CCPA") was enacted to protect consumers' personal information, and to give consumers more control over the personal information that businesses collect about them. As of January 1, 2023, under the CCPA, consumers have the "right to limit the use and disclosure of sensitive

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

personal information collected about them."[32]

151. Members of the Class are consumers within the meaning of the CCPA. Cal. Civ. Code § 1798.140(i).

152. EP is a business within the meaning of the CCPA, because it is a "limited liability company . . . organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information," which on information and belief had gross revenues in excess of $25 million dollars in 2022.[33] CCPA. Cal. Civ. Code § 1798.140(d)(1).

153. The information compromised in the Data Breach constitutes "personal information" as defined under the CCPA. Cal. Civ. Code § 1798.140(v)(1). As disclosed by EP, that information included full names, mailing addresses, and Social Security numbers and/or tax identification numbers.

154. Through the above-detailed conduct, EP violated the CCPA § 1798.150(a)(1) by, *inter alia,* failing to implement and maintain reasonable data security procedures and practices appropriate to the information that it stored.

155. EP's failure to implement reasonable data security practices and procedures, and to prevent the Data Breach and exfiltration of Plaintiff's and Class Members' PII, constitutes a breach of its duty under the CCPA.

156. As a result of the Data Preach, Plaintiff's and Class Members unredacted and unencrypted PII was subject to unauthorized access, exfiltration, and theft.

[32] California Consumer Privacy Act, State of California Dep't of Just.: Office of the Attorney General, https://oag.ca.gov/privacy/ccpa#:~:text=The%20CCPA%20applies%20to%20for,%2C%20households%2C%20or%20devices%3B%20or (last visited Aug. 30, 2023).

[33] Entertainment Partners, ZoomInfo https://www.zoominfo.com/c/entertainment-partners/49385009#:~:text=Entertainment%20Partners's%20revenue%20is%20%24194.2%20Million%20What%20is%20Entertainment%20Partners's%20SIC%20code%3F (last visited Aug. 30, 2023).

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

EIGHTH CAUSE OF ACTION
Violations of California's Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq.*

157. On behalf of Plaintiff and the Nationwide Class, Plaintiff repeats and realleges Paragraphs 1-90 as if fully alleged herein.

158. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

159. EP engaged in unlawful activity prohibited by the UCL. The actions of EP as alleged herein constitute unlawful and unfair business practices within the meaning of the UCL.

160. EP violated the "unlawful" prong of the UCL by violating, *inter alia*, Plaintiff's and Class Members' constitutional rights to privacy and state consumer protection statutes, such as California's Consumer Privacy Act, Section 5 of the FTC Act, and Article 1, Section 1 of the California Constitution. Plaintiff and Class Members reserve the right to allege other violations of law by EP. EP's wrongful actions, omissions, and want of ordinary care, alleged herein, are ongoing and continue to date of the present filing.

161. EP also violated the UCL by failing to timely notify Plaintiff and Class Members pursuant to Cal. Civ. Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate and timely fashion, they could have taken precautions to safeguard and protect their PII and identities.

162. EP's acts, omissions, and conduct also violate the "unfair" prong of the UCL because those acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and Class Members. The harm caused by EP's conduct outweighs any potential benefits attributable to such conduct, and there were reasonably available alternatives to further EP's legitimate business

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

interests, other than EP's conduct described herein.

163. By exposing and compromising Plaintiff's and Class Members' PII without authorization, EP engaged in a fraudulent business practice that is likely to deceive a reasonable consumer.

164. A reasonable person would not have provided PII to EP had he or she known the truth about EP's practices alleged herein. By withholding material information about its practices, EP was able to convince clients and customers to use its financial services and provide highly valuable PII to EP. Accordingly, EP's conduct was also "fraudulent" within the meaning of the UCL.

165. As a result of EP's violations of the UCL, Plaintiff and Class Members are entitled to injunctive relief.

166. As a result of EP's violations of the UCL, Plaintiff and Class Members have suffered injury in fact and lost money or property, as detailed above. Plaintiff requests that the Court issue sufficient equitable relief to restore Plaintiff and Class Members to the position they would have been in had EP not engaged in unfair competition.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of himself and all others similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and,

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

DATED: September 14, 2023 **PEARSON WARSHAW, LLP**

By: */s/ Daniel L. Warshaw*
DANIEL L. WARSHAW

DANIEL L. WARSHAW (Bar No. 185365)
dwarshaw@pwfirm.com
PEARSON WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, California 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

JAMES J. PIZZIRUSSO*
jpizzirusso@hausfeld.com
AMANDA V. BOLTAX*
mboltax@hausfeld.com
HAUSFELD LLP
888 16th Street, NW, Suite 300
Washington, D.C. 20006
Telephone: (202) 542-7200
Facsimile: (202) 542-7201

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

STEVEN M. NATHAN (Bar No. 153250)
snathan@hausfeld.com
HAUSFELD LLP
33 Whitehall Street, 14th Floor
New York, NY 10004
Telephone: (646) 357-1100
Facsimile: (212) 202-4322

PAUL R. KIESEL (Bar No. 119854)
kiesel@kiesel.law
JEFFREY A. KONCIUS (Bar No. 189803)
koncius@kiesel.law
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Telephone: (310) 854-4444
Facsimile: (310) 854-0812

Counsel for Plaintiff and the Proposed Class

**Pro Hac Vice Forthcoming*

PEARSON WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403